

Ipad & Mac Users Class

PHISHING & SCAMS

What is Phishing?

It's the fraudulent practice of sending emails purporting to be from reputable companies and organisations in order to induce people to reveal personal information, such as login details passwords and credit card numbers, online.

Here is example of a phishing email scan and message might look like.

" Hello

*As part of our security measures we regularly screen activity in the Facebook system.
We are contacting you after noticing an issue on your account*

*Our system detected unusual Copyrights activity linked to your Facebook account,
please follow the link bellow to fill the Copyright Law form.*

http://www.facebook.com/application_form

EMAIL LINK

SPELLING

Note if you don't fill the application your account will be permanently blocked

THREAT
S

Regards

Facebook Copyrights Department"

A OMMON DEPARTMENT or PERSON

LOOK FOR

- **Spelling and bad grammar.** Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam. For more information, see [Email and web scams: How to help protect yourself](#).
- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address. Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

<https://www.woodgrovebank.com/loginscript/user2.jsp>

<http://192.168.255.205/wood/index.htm>

- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised. For more information, [Watch out for fake alerts](#).
- **Using popular websites or companies, like banks, electricity etc** Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.

TASK

1. Look up the meaning of related “**spear phishing**” as related to phishing not fishing
2. Visit the se sites to inform your self about phishing
Use SCAM WATCH <https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams>

<https://www.scamwatch.gov.au/types-of-scams>

<https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information>

<https://www.scamwatch.gov.au>

3. LOOKING AT PHISHING EXAMPLES

<https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2>

<https://www.onguardonline.gov/phishing#examples%20of%20phishing%20messages>